UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/653,500	09/02/2003	Len L. Mizrah	AIDT 1006-1	3755

22470 7590 03/29/2007
HAYNES BEFFEL & WOLFELD LLP
P O BOX 366
HALF MOON BAY, CA 94019

EXAMINER	
DINH, MINH	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/653,500	MIZRAH, LEN L.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) *5-7,14-16 and 23-25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,8-13,17-22,26 and 27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/24/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. This application contains claims directed to the following patentably distinct species: (a) a species of data veiling process using Byte-Veil-Unveil (ByteVU) algorithm as disclosed in figure 5; (b) a species of data veiling process using Bit-Veil-Unveil (BitVU) algorithm as disclosed in figure 6; and (c) a species of data veiling process using Byte-Bit-Veil-Unveil (BBVU) algorithm as disclosed in figure 7. The species are distinct because: the specification discloses that they are mutually exclusive, i.e., one but not all three algorithms is used (paragraph 0029); and, according to the corresponding figures, they are not obvious variants, and they have a materially different design, mode of operation or function.

Applicant is required under 35 U.S.C. 121 to elect a single disclosed species for prosecution on the merits to which the claims shall be restricted if no generic claim is finally held to be allowable. Currently, claims 1-3, 8-12, 17-21 and 26-27 are generic.

Applicant is advised that a reply to this requirement must include an identification of the species that is elected consonant with this requirement, and a listing of all claims readable thereon, including any claims subsequently added. An argument that a claim is allowable or that all claims are generic is considered nonresponsive unless accompanied by an election.

Upon the allowance of a generic claim, applicant will be entitled to consideration of claims to additional species which depend from or otherwise require all the limitations of an allowable generic claim as provided by 37 CFR 1.141. If claims are added after the election, applicant must indicate which are readable upon the elected species. MPEP § 809.02(a).

2. During a telephone conversation with Mark Haynes on 2/5/07 a provisional election was made with traverse to prosecute species (a), which corresponds to claims 4, 13 and 22. Affirmation of this election must be made by applicant in replying to this Office action. Claims 5-7, 14-16 and 23-25 are withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Specification

3. It is requested that Applicant provide the application/patent numbers of related applications listed in paragraphs 1-2 that might not have been available at the time of filing. Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-4, 8-13, 17-22 and 26-27 are rejected under 35 U.S.C. 101 because they are not directed to a practical application. A practical application would be established by a useful, concrete and tangible result. For a claim to provide a tangible result, it must produce a result that is limited to having a real world value rather than a result that may be interpreted to be abstract in nature as, for example, a thought, a computation, or manipulated data. Claim 1 is directed to a method for performing mutual authentication between a first station and a second station whereby the first station uses a shared secret to produce a challenge and sends the challenge to the second station, and the second station uses the shared secret to process the challenge and replies with a response. However, the claimed subject matter does not produce a tangible result because the claim does not recite any step(s) for the first station to determine the authenticity of the second station, i.e., by comparing the reply with an expected value to see if they match. Therefore, the claim is not directed to a practical application. Claims 10 and 19 are rejected on the

same basis as claim 1. Claims that are not specifically addressed are rejected by virtue of their dependency.

6. Claims 1-4, 8-13, 17-22 and 26-27 are rejected under 35 U.S.C. 101 because they are not directed to a practical application. A practical application would be established by a useful, concrete and tangible result. For a claim to provide a tangible result, it must produce a result that is limited to having a real world value rather than a result that may be interpreted to be abstract in nature as, for example, a thought, a computation, or manipulated data. Claim 1 is directed to a method for performing mutual authentication between a first station and a second station whereby the first station uses a shared secret to produce a challenge and sends the challenge to the second station, and the second station uses the shared secret to process the challenge and replies with a response. However, the claimed subject matter does not produce a tangible result because the claim does not recite any step(s) for the second station to authenticate the first station, i.e., the second station does not send a challenge to the first station and receive any response to the challenge from the first station. Therefore, the claim is not directed to a practical application. Claims 10 and 19 are rejected on the same basis as claim 1.

Claims that are not specifically addressed are rejected by virtue of their dependency.

7. Claims 1-4, 8-13, 17-22 and 26-27 are rejected under 35 U.S.C. 101 because they are not directed to a useful process. Claim 1 is directed to a method for performing mutual authentication between a first station and a second station. The disclosure (Specification, paragraphs 0019, 0071; figure 3, step 5 through step n+2; figures 8A-B) discloses that an iterative sequence of encrypted messages from the server to the client and back to the server is performed in order to complete mutual authentication. However, the claim recites only one sequence of messages, i.e., the first station sends a message to the second station, and the second station sends a reply message to the first station. Since the claim does not recite an iterative sequence of messages is performed, the method is incomplete and, therefore, not a useful method. Claims 10 and 19 are rejected on the same basis as claim 1. Claims that are not specifically addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1-4, 8-13, 17-22 and 26-27 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. Regarding claim 1, the omitted steps are: determining if the version of the particular data random key is correct at the first station (figure 3, step 6 through step n+2, see beginning of each step). Without comparing the reply with an expected value to see if they match, the first station would not be able to determine the authenticity of the second station. Claims 10 and 19 are rejected on the same basis as claim 1. Claims that are not specifically addressed are rejected by virtue of their dependency.

10. Claims 1-4, 8-13, 17-22 and 26-27 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. Regarding claim 1, the omitted steps are: determining, at the second station, if a particular data random key received from the first station is correct (figure 3, step n+1). Without comparing a reply from the first station with an expected value to see if they match, the second station would not be able to determine the authenticity of the first station. Claims 10 and 19 are rejected on the same basis as claim 1. Claims that are not specifically addressed are rejected by virtue of their dependency.

11. Claims 1-4, 8-13, 17-22 and 26-27 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. Regarding claim 1, the omitted steps are: the steps of encrypting, sending and receiving are performed iteratively and for each time, a different data random key is encrypted using a different share secret. The disclosure discloses that an iterative sequence of messages from the server to the client and back to the server is performed in order to complete mutual authentication (Specification, paragraphs 0019, 0071; figure 3, step 5 through step n+2; figures 8A-B).

12. Claim 21 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 21, which depends on claim 19, recites the limitation "said additional particular data random key" in line 1. There is insufficient antecedent basis for this limitation in the claim. For examination purpose, claim 21 is considered as a dependent claim of claim 20.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 1, 8-10, 17-19 and 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al. (5,241,599) in view of "FIPS 46-3 Data Encryption Standard (DES)" (hereinafter "FIPS 46-3"). Bellovin discloses a method and system for performing mutual authentication between a first station (i.e., entity Alice) and a second station (i.e., entity Bob) by executing an interactive exchange of messages comprising: encrypting a particular data random value (i.e., challenge A), which meets the limitation of a random data key, at the first station using a shared secret to produce a first encrypted value, where access to the shared secret indicates authenticity of the first station; sending a first message to the second station including the first encrypted value (fig. 2, step 221), where the second station decrypts said particular data random value using the shared secret, and where the second station encrypts a hashed version of the particular data random key using the shared secret to produce a second encrypted value, and sends a second message to the first station carrying

the second encrypted key (fig. 2, step 227; col. 7, lines 27-34), where access to the shared secret indicates authenticity of the second station; and receiving the second message, and decrypting the version of the particular data random value at the first station (col. 7, lines 11-13).

Bellovin discloses encrypting a value only one time (either the random value or the version of the random value) to produce an encrypted value for transmission. Bellovin does not disclose encrypting the value multiple times. FIPS 46-3 discloses performing multiple DES encryption (i.e., Triple DES) on data, wherein single DES encryption veils (i.e., conceals) data using a conversion array seeded by a shared secret, i.e., performing substitution and permutation functions on key data (Section 15 – Qualifications; figure 3). It would have been obvious to one of ordinary in the art at the time the invention was made to modify Bellovin method to perform multiple DES encryption to the value, as taught by FIPS 46-3, to increase security.

15. Claims 1, 9-10, 18-19 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al. (6,920,559) in view of "FIPS 46-3 Data Encryption Standard (DES)" (hereinafter "FIPS 46-3"). Nessett discloses a method and system for performing mutual authentication between a first station (i.e., AP2) and a second station (i.e., WC) by executing an interactive exchange of messages comprising: encrypting a

particular data random value (i.e., C1), which meets the limitation of a random data key, at the first station using a shared secret to produce a first encrypted value (fig. 4B, step 460), where access to the shared secret indicates authenticity of the first station; sending a first message to the second station including the first encrypted value (fig. 4B, step 463), where the second station decrypts said particular data random value using the shared secret (fig. 4B, step 466), and where the second station encrypts a version of the particular data random key using the shared secret to produce a second encrypted value (fig. 4B, step 472), and sends a second message to the first station carrying the second encrypted key (fig. 4B, step 475), where access to the shared secret indicates authenticity of the second station; and receiving the second message, and decrypting the version of the particular data random value at the first station (fig. 4C, step 478).

Nessett discloses encrypting a value only one time (either the random value or the version of the random value) to produce an encrypted value for transmission. Nessett does not disclose encrypting the value multiple times. FIPS 46-3 discloses performing multiple DES encryption (i.e., Triple DES) on data, wherein single DES encryption veils (i.e., conceals) data using a conversion array seeded by a shared secret, i.e., performing substitution and permutation functions on key data (Section 15 – Qualifications; figure 3). It would have been obvious to one of ordinary in the art at the time the

invention was made to modify Nessett method to perform multiple DES encryption to the value, as taught by FIPS 46-3, to increase security.

Double Patenting

16. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

17. Claims 1-2, 10-11 and 19-20 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 15, 40 and 65 of copending Application No. 10/653,506. Although the conflicting claims are not identical, they are not patentably distinct from each other because claims 15, 40 and 65 of copending

Application '506 contain(s) every element of claims 1, 10 and 19 of the instant application and as such anticipate(s) claims 1, 10 and 19 of the instant application.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Allowable Subject Matter

18. Subject to the above 101, 112, second paragraph, and double patenting rejections, claims 2-4, 11-13 and 20-22 would be allowable over the prior art of record.

19. The following is a statement of reasons for the indication of allowable subject matter. The present invention is directed to a method and system for performing mutual authentication between a first station and a second station wherein the first station veils a random key using a first conversion array seeded by a shared secret, encrypts the veiled random key and sends the encrypted key to the second station; the second station first decrypts and unveils the random key using the shared secret, and then veils a version of the random key using a second conversion array seeded by the shared secret, encrypts the veiled version of the random key and sends the

encrypted veiled version of the random key to the first station; the first station then decrypts and unveils the version of the random key.

More specifically, dependent claims 2, 11 and 20 identify the uniquely distinct features: performing the same process by the first and second stations (the same steps in the same order) to an additional random key. The closest prior art include: (a) Bellovin et al. (5,241,599) teaches a method for mutual authentication between a first entity and second entity wherein the first entity encrypts a random value using a shared secret, sends the encrypted random value to the second entity; the second entity decrypts the random value, encrypts a version of the random value using the shared secret and sends the encrypted version of the random data to the first entity, who then decrypts the version of the random data; (b) Nessett et al. (6,920,559) teaches a method for mutual authentication similar to that of Bellovin; and (c) "FIPS 46-3 Data Encryption Standard (DES)" teaches performing multiple DES encryption (i.e., Triple DES) on data, wherein single DES encryption veils (i.e., conceals) data using a conversion array seeded by a shared secret. However, Bellovin, Nessett, and "FIPS 46-3", either alone or in combination, do not teach the specific features mentioned above.

Dependent claims 4, 13 and 22 identify the uniquely distinct features: one the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and generating one of

the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and placing a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values. The closest prior art include: (a) "FIPS 46-3 Data Encryption Standard (DES)" teaches using a conversion array seeded by a shared secret for veiling data in DES; and (b) Stallings ("Cryptography and Network Security – Principles And Practice") also teaches using a conversion array seeded by a shared secret for veiling data in AES (Advanced Encryption Standard). However, "FIPS 46-3" and Stalling, either alone or in combination, do not teach the specific features mentioned above.

The prior art, taken either singly or in combination, fails to anticipate or fairly suggest the limitations of applicant's independent claim, in such a manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claims are therefore considered to be in condition for allowance as being novel and nonobvious over prior art.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 7,069,438 to Balabine et al.

Kaufman et al., "Network Security – Private Communication in a Public World"

Li et al., "An Improved Key Distribution Protocol with Perfect Reparability"

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MD

Minh Dinh
Examiner
Art Unit 2132

3/20/07

Benjamin E. Lanier
Examiner AU 2132